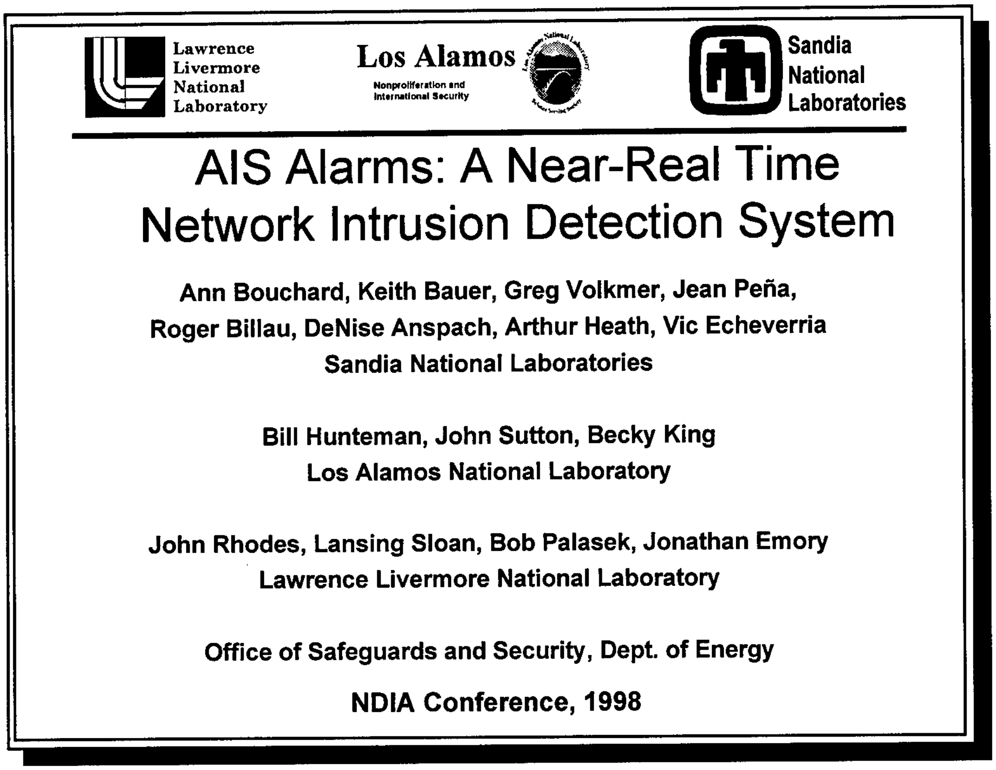


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

AIS Alarms: A Near-Real Time Network Intrusion Detection System

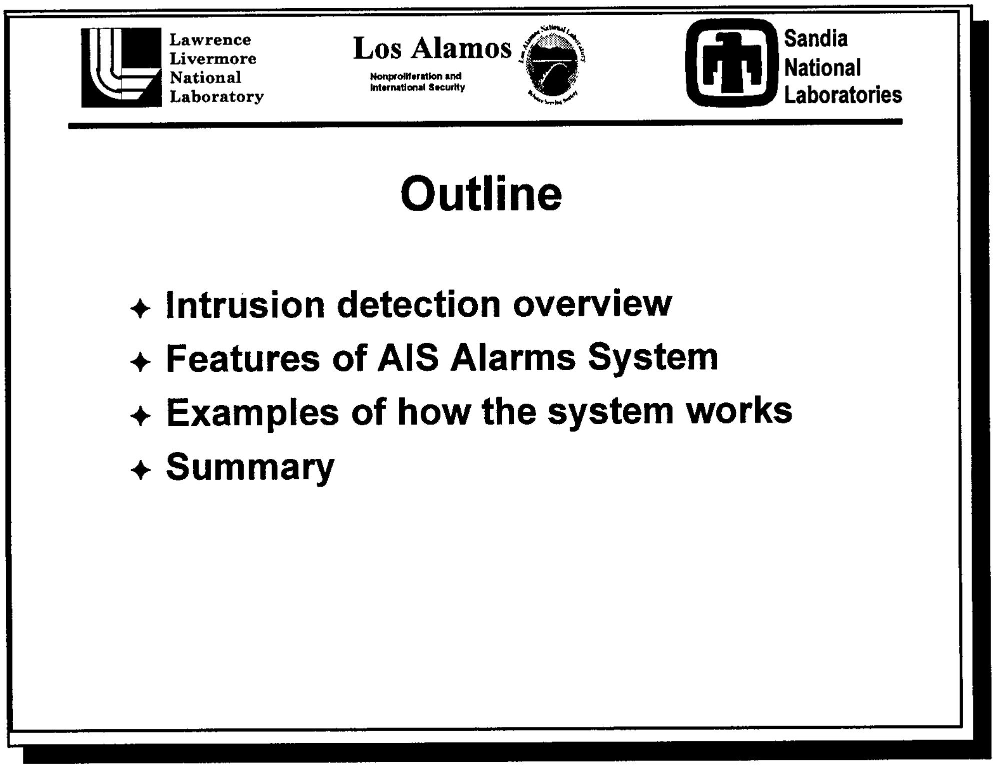
Ann Bouchard, Keith Bauer, Greg Volkmer, Jean Peña,
Roger Billau, DeNise Anspach, Arthur Heath, Vic Echeverria
Sandia National Laboratories

Bill Hunteman, John Sutton, Becky King
Los Alamos National Laboratory

John Rhodes, Lansing Sloan, Bob Palasek, Jonathan Emory
Lawrence Livermore National Laboratory

Office of Safeguards and Security, Dept. of Energy

NDIA Conference, 1998



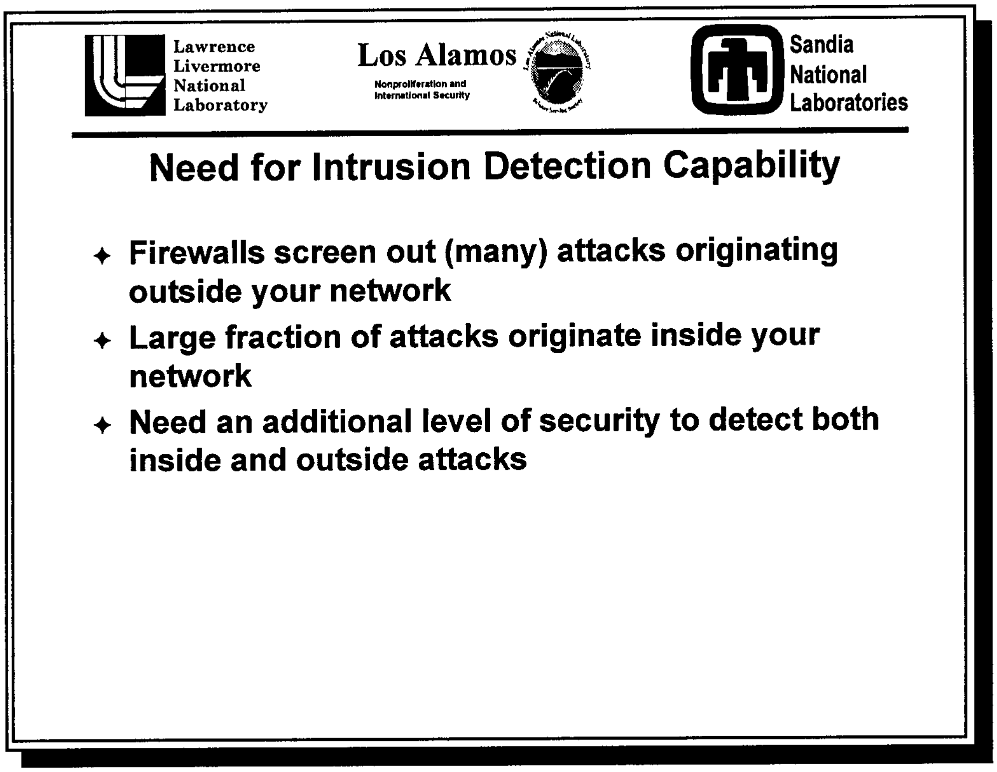
Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Outline

- Intrusion detection overview
- Features of AIS Alarms System
- Examples of how the system works
- Summary



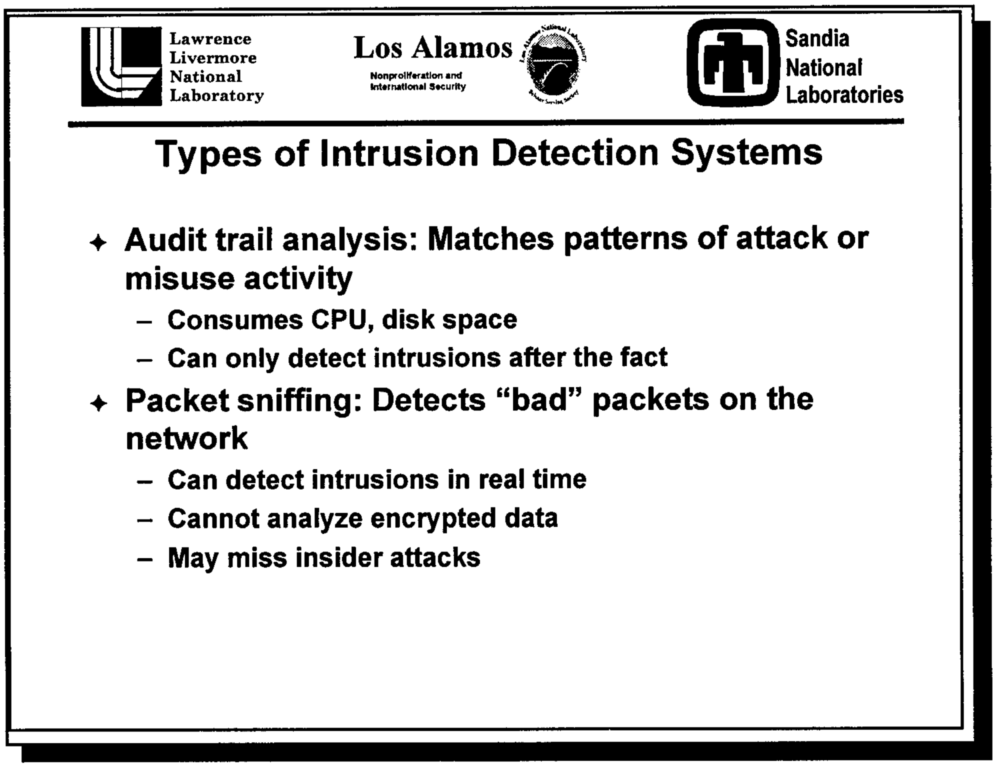
Lawrence
Livermore
National
Laboratory

Los Alamos
Nonproliferation and
International Security

Sandia
National
Laboratories

Need for Intrusion Detection Capability

- ✦ Firewalls screen out (many) attacks originating outside your network
- ✦ Large fraction of attacks originate inside your network
- ✦ Need an additional level of security to detect both inside and outside attacks



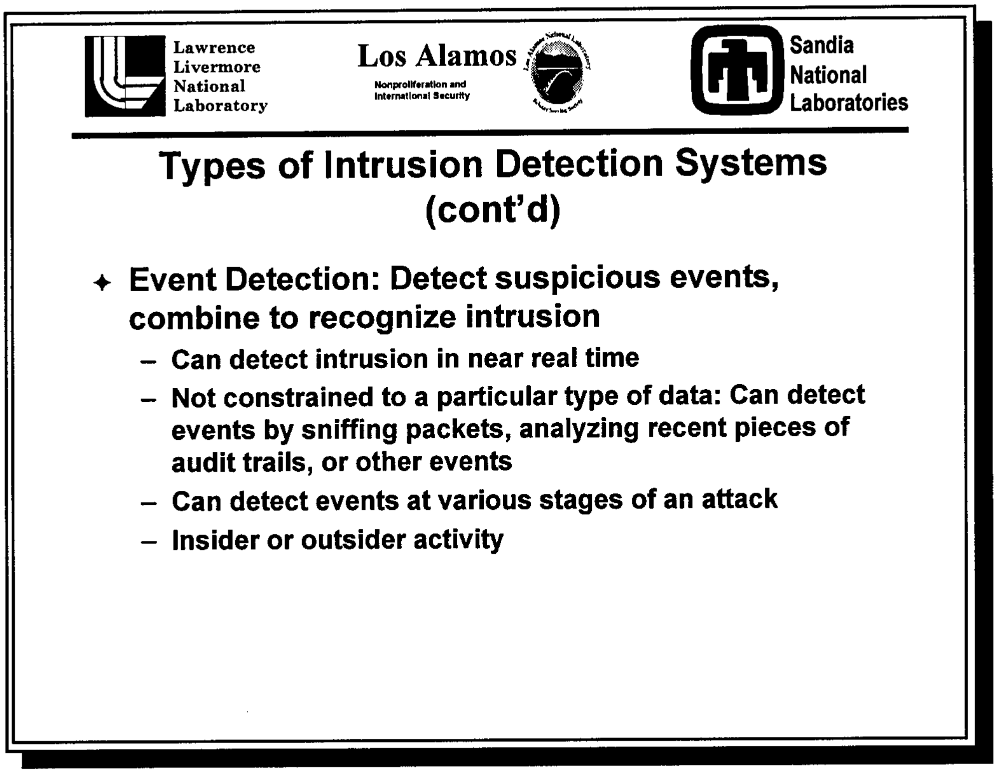
Lawrence
Livermore
National
Laboratory

Los Alamos
Nonproliferation and
International Security

Sandia
National
Laboratories

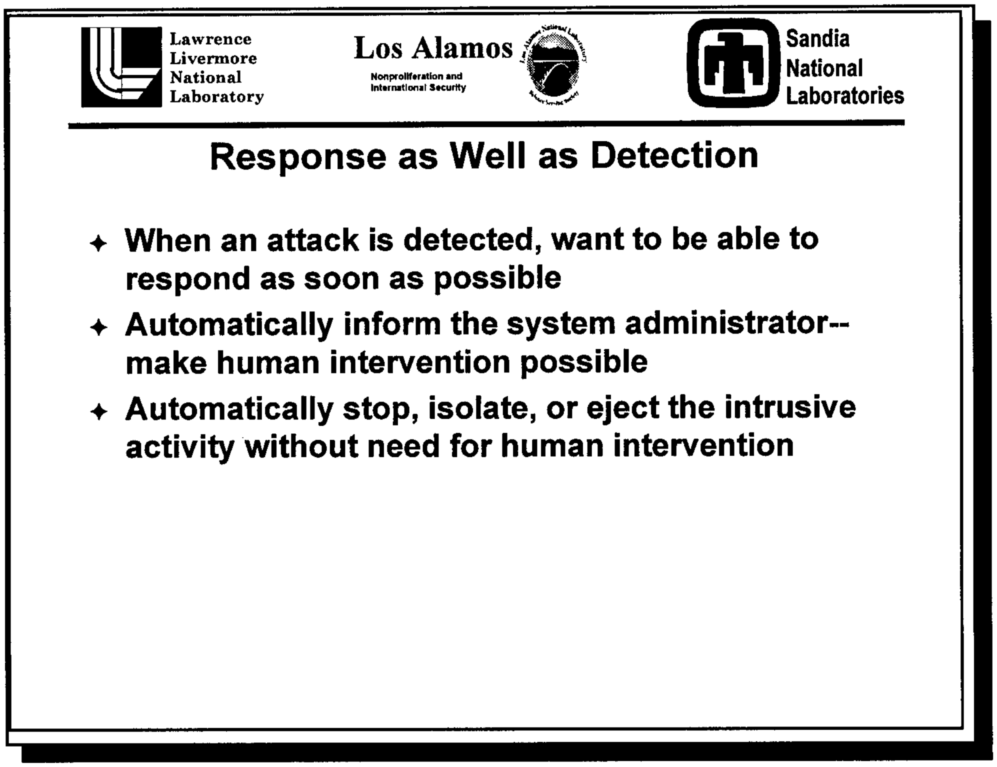
Types of Intrusion Detection Systems

- ✦ Audit trail analysis: Matches patterns of attack or misuse activity
  - Consumes CPU, disk space
  - Can only detect intrusions after the fact
- ✦ Packet sniffing: Detects "bad" packets on the network
  - Can detect intrusions in real time
  - Cannot analyze encrypted data
  - May miss insider attacks



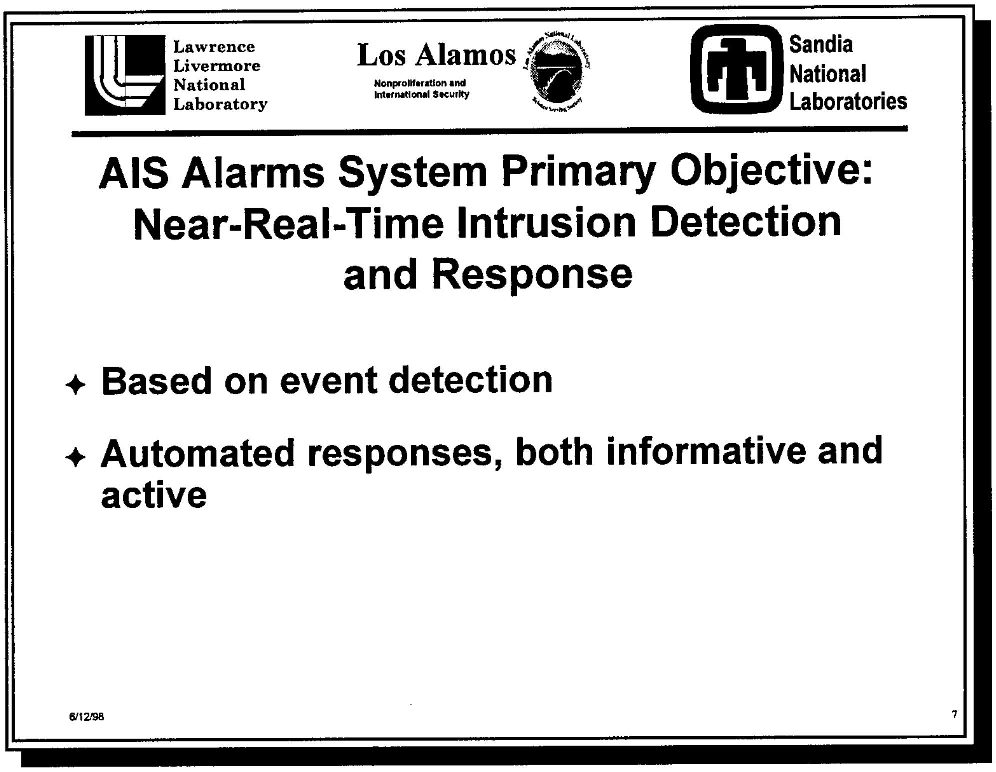
Types of Intrusion Detection Systems (cont'd)

- Event Detection: Detect suspicious events, combine to recognize intrusion
  - Can detect intrusion in near real time
  - Not constrained to a particular type of data: Can detect events by sniffing packets, analyzing recent pieces of audit trails, or other events
  - Can detect events at various stages of an attack
  - Insider or outsider activity



Response as Well as Detection

- When an attack is detected, want to be able to respond as soon as possible
- Automatically inform the system administrator--make human intervention possible
- Automatically stop, isolate, or eject the intrusive activity without need for human intervention



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

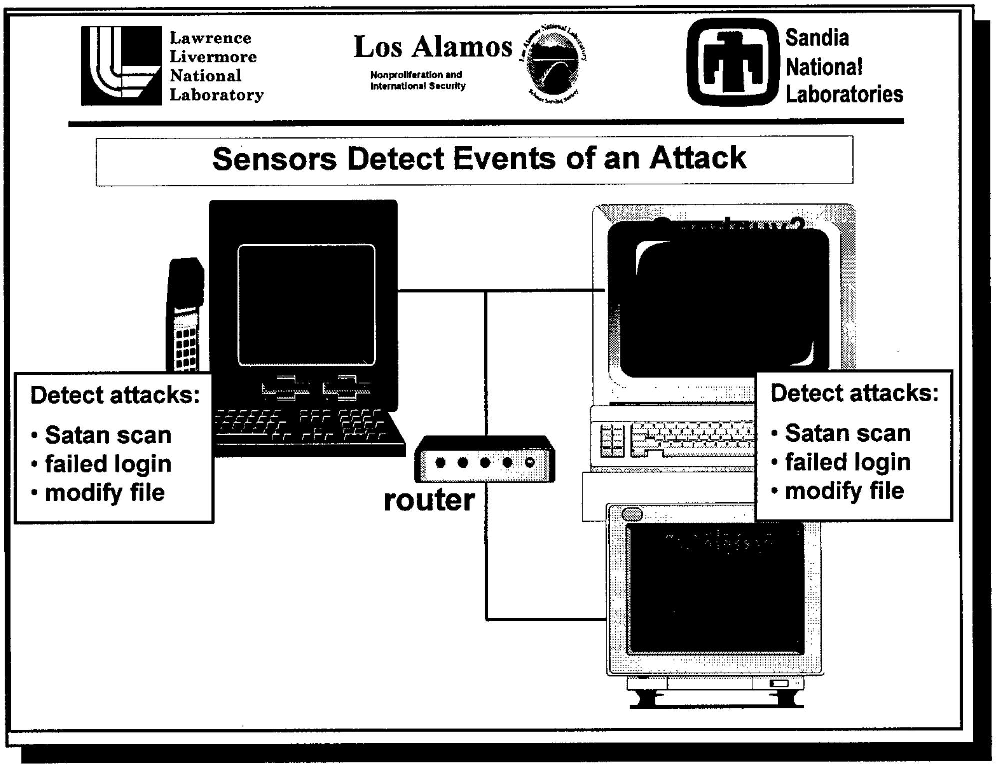
Sandia National Laboratories

AIS Alarms System Primary Objective: Near-Real-Time Intrusion Detection and Response

- Based on event detection
- Automated responses, both informative and active

6/12/98

7



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

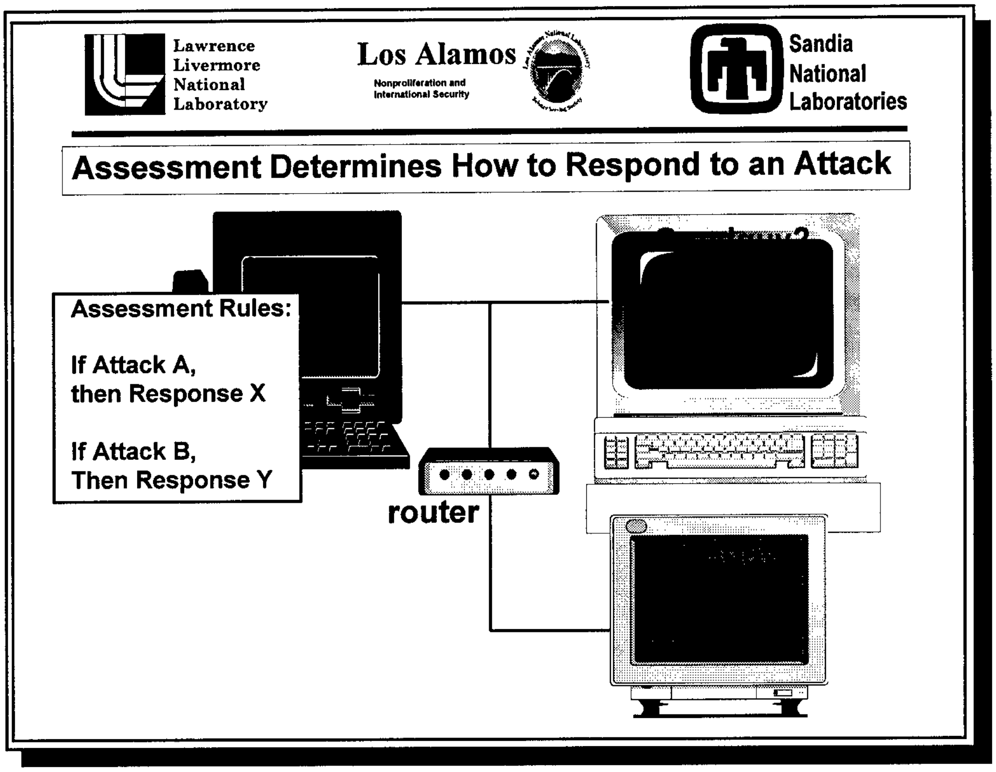
Sandia National Laboratories

Sensors Detect Events of an Attack

Detect attacks:
- Satan scan
- failed login
- modify file

router

Detect attacks:
- Satan scan
- failed login
- modify file



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

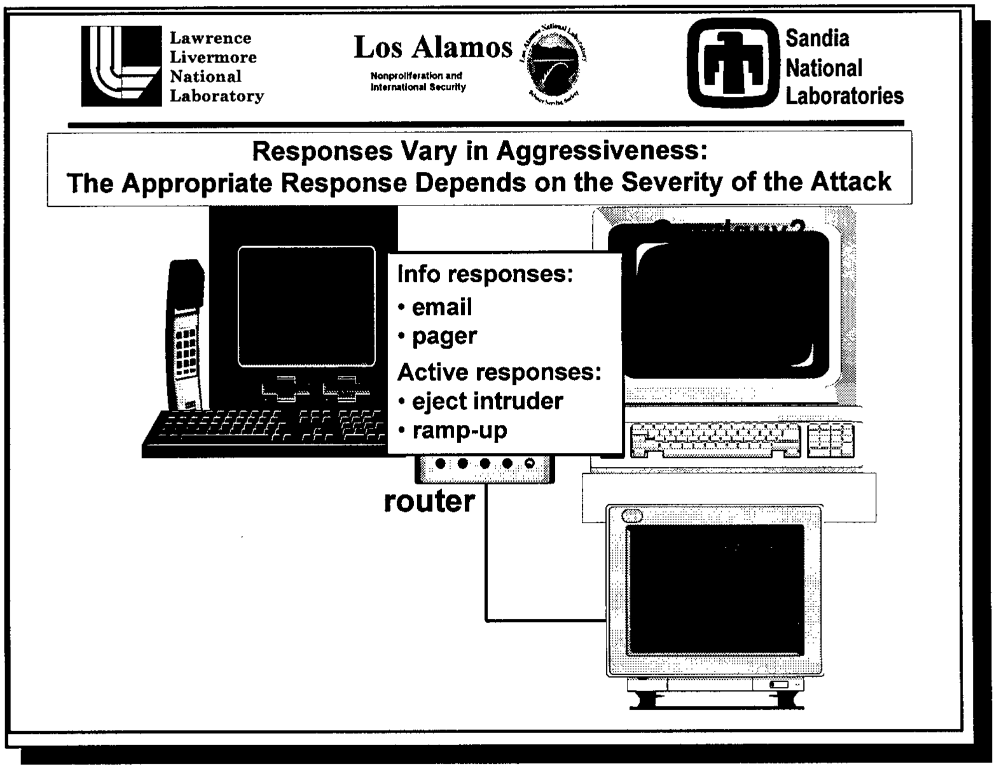
Sandia National Laboratories

Assessment Determines How to Respond to an Attack

Assessment Rules:

If Attack A,
then Response X

If Attack B,
Then Response Y



Lawrence Livermore National Laboratory

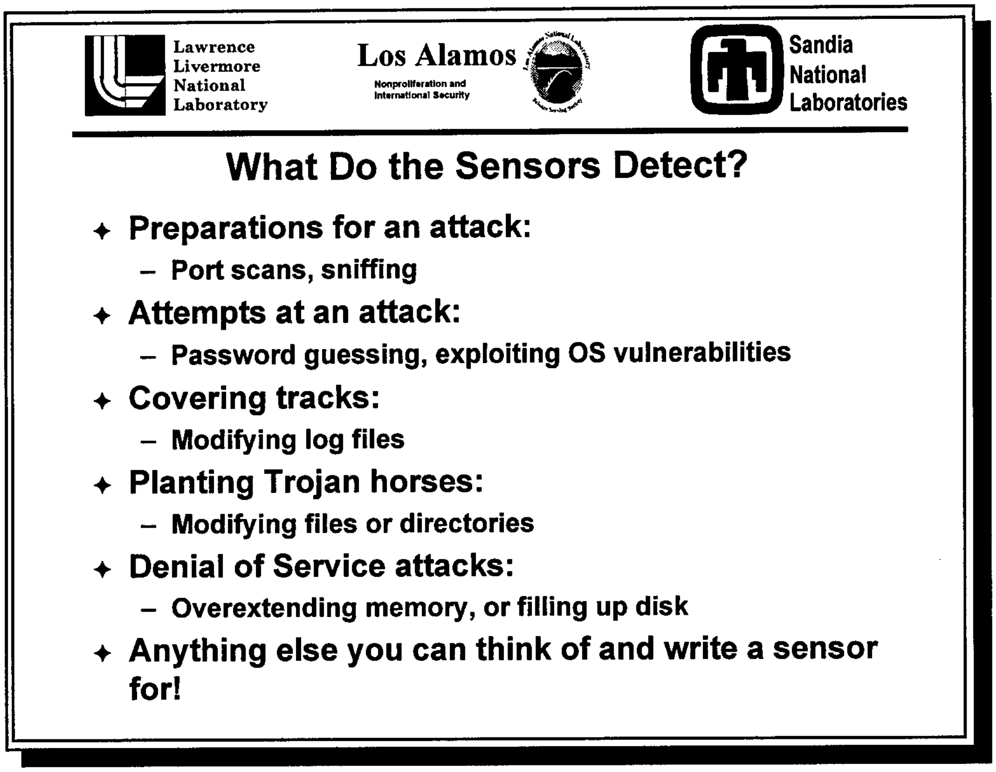
Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Responses Vary in Aggressiveness: The Appropriate Response Depends on the Severity of the Attack

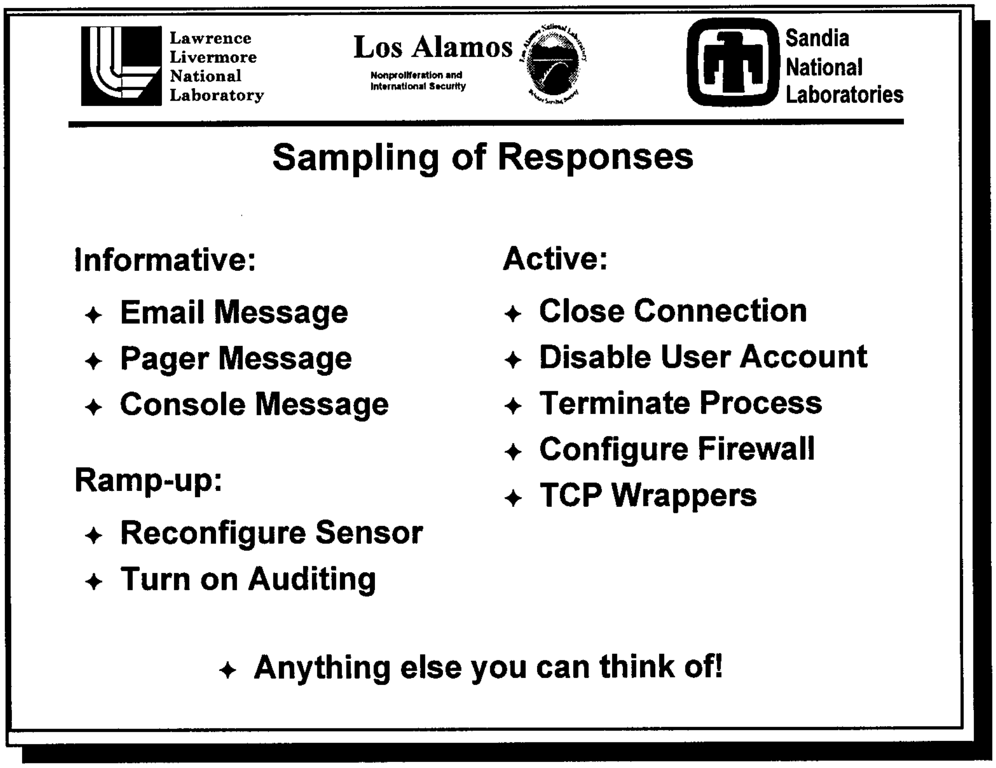
Info responses:
- email
- pager

Active responses:
- eject intruder
- ramp-up



What Do the Sensors Detect?

- Preparations for an attack:
  - Port scans, sniffing
- Attempts at an attack:
  - Password guessing, exploiting OS vulnerabilities
- Covering tracks:
  - Modifying log files
- Planting Trojan horses:
  - Modifying files or directories
- Denial of Service attacks:
  - Overextending memory, or filling up disk
- Anything else you can think of and write a sensor for!



Sampling of Responses

Informative:

- Email Message
- Pager Message
- Console Message

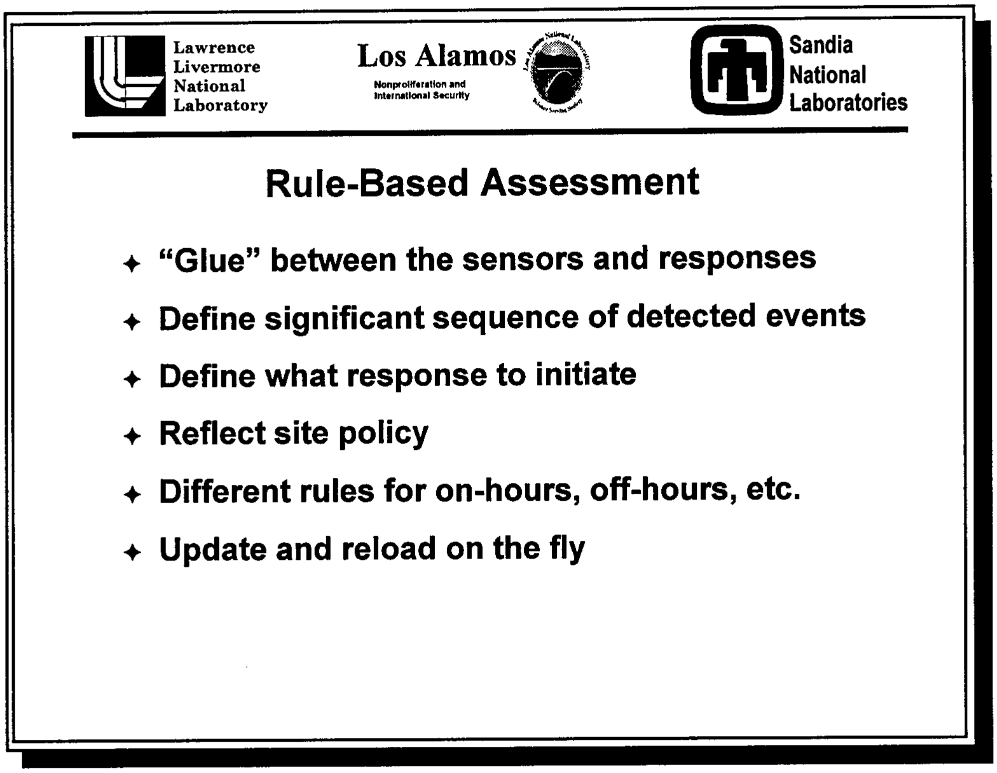
Ramp-up:

- Reconfigure Sensor
- Turn on Auditing

Active:

- Close Connection
- Disable User Account
- Terminate Process
- Configure Firewall
- TCP Wrappers

- Anything else you can think of!



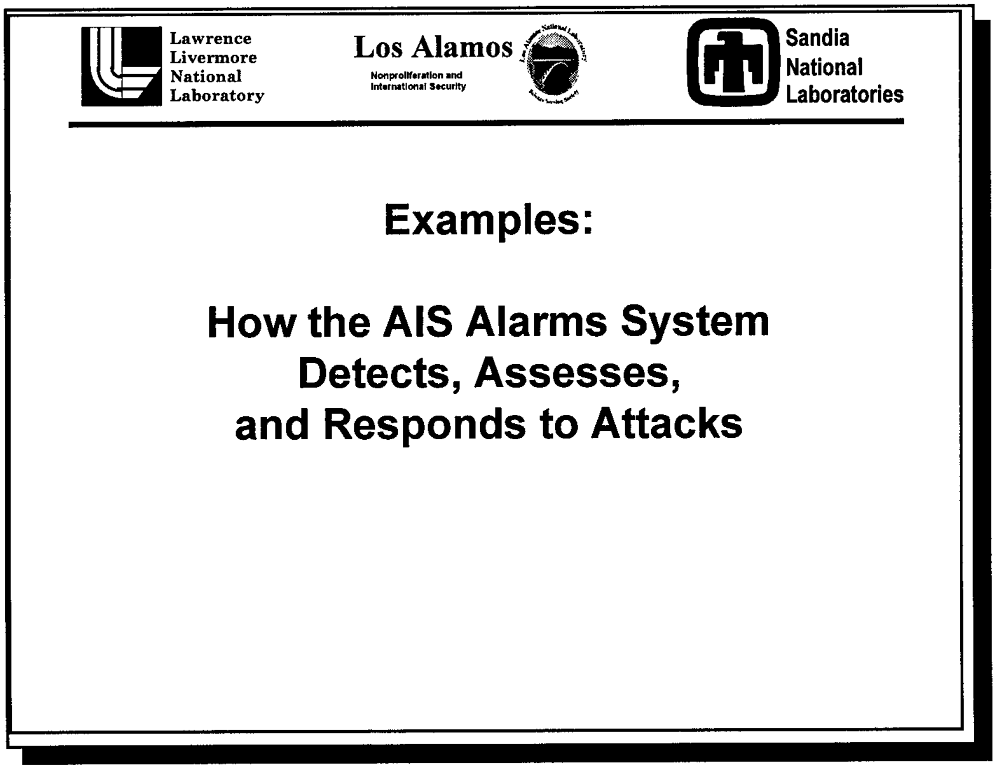
Lawrence Livermore National Laboratory

Los Alamos Nonproliferation and International Security

Sandia National Laboratories

Rule-Based Assessment

- "Glue" between the sensors and responses
- Define significant sequence of detected events
- Define what response to initiate
- Reflect site policy
- Different rules for on-hours, off-hours, etc.
- Update and reload on the fly



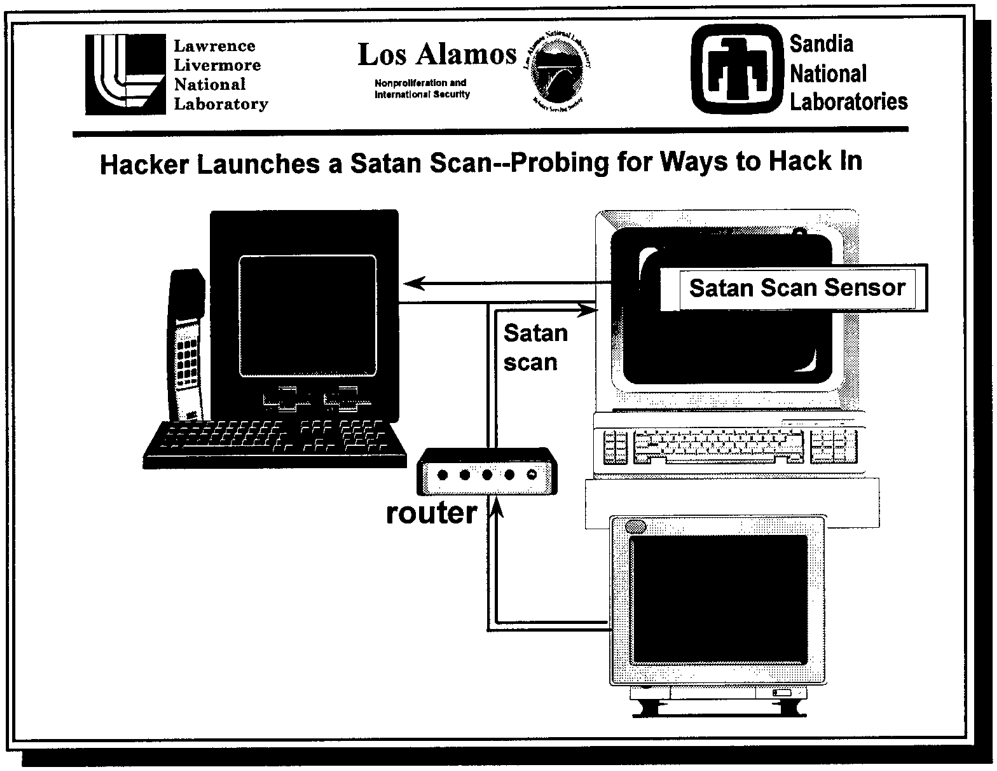
Lawrence Livermore National Laboratory

Los Alamos Nonproliferation and International Security

Sandia National Laboratories

Examples:

How the AIS Alarms System Detects, Assesses, and Responds to Attacks

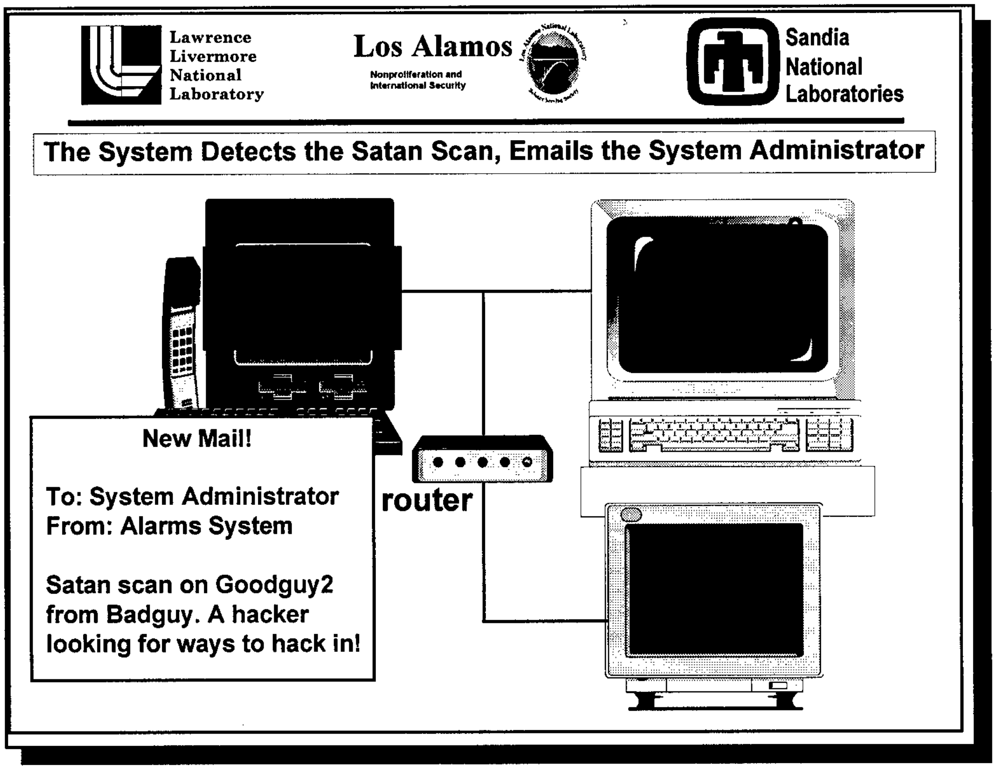


Lawrence Livermore National Laboratory

Los Alamos Nonproliferation and International Security

Sandia National Laboratories

Hacker Launches a Satan Scan--Probing for Ways to Hack In



Lawrence Livermore National Laboratory

Los Alamos Nonproliferation and International Security

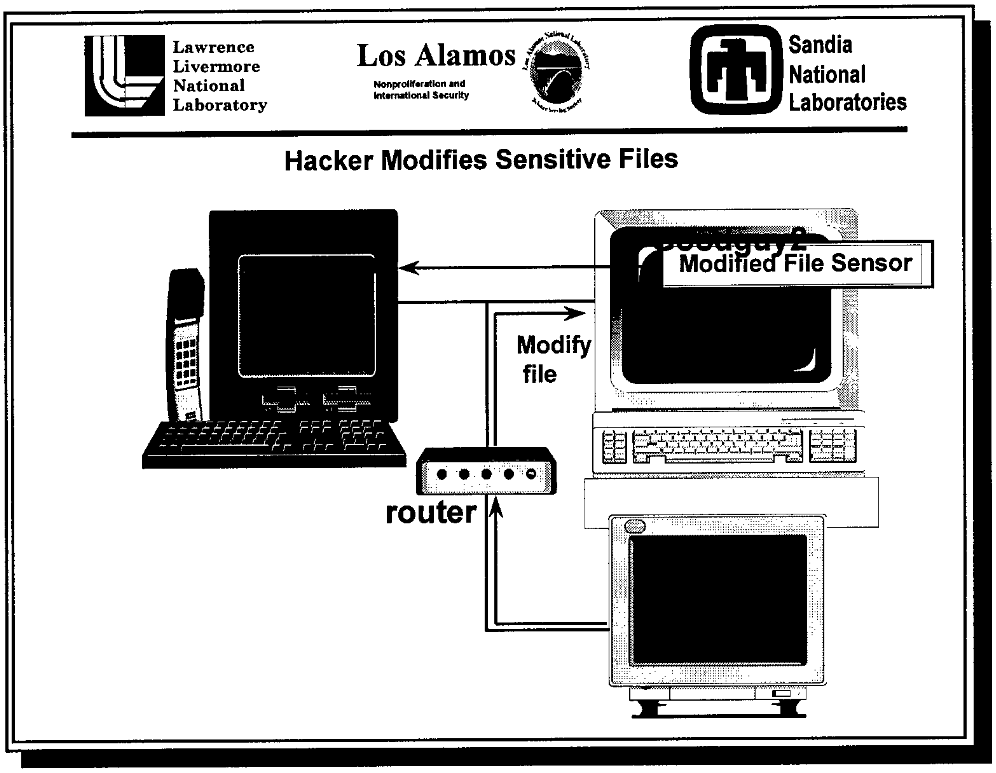
Sandia National Laboratories

The System Detects the Satan Scan, Emails the System Administrator

New Mail!

To: System Administrator
From: Alarms System

Satan scan on Goodguy2 from Badguy. A hacker looking for ways to hack in!

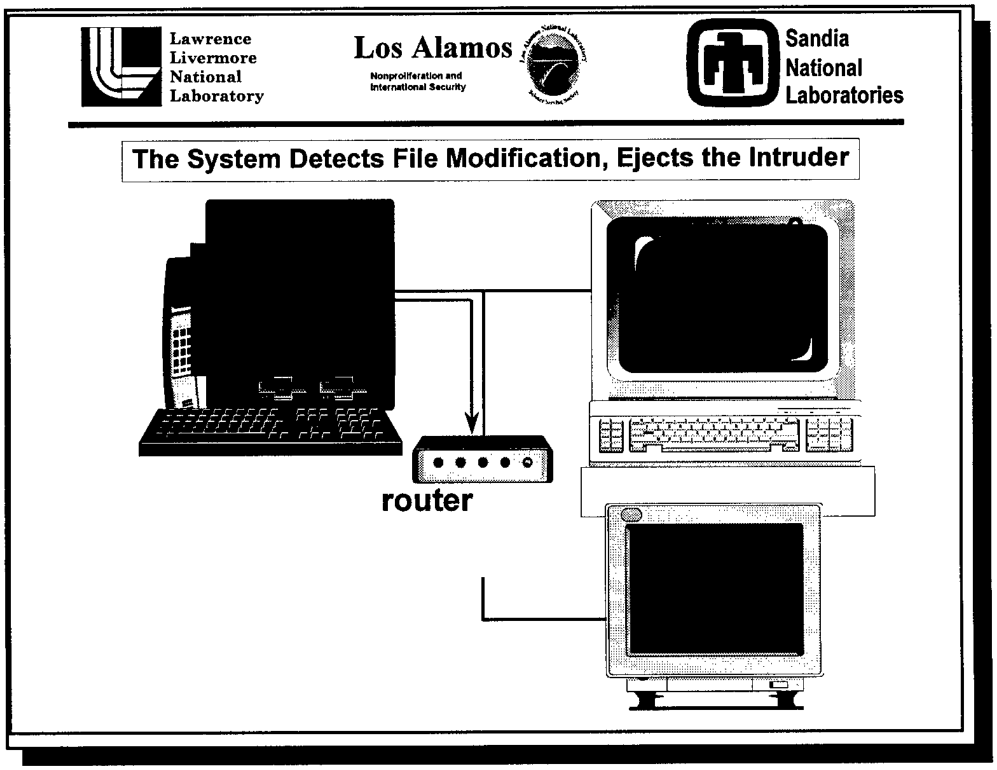


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Hacker Modifies Sensitive Files

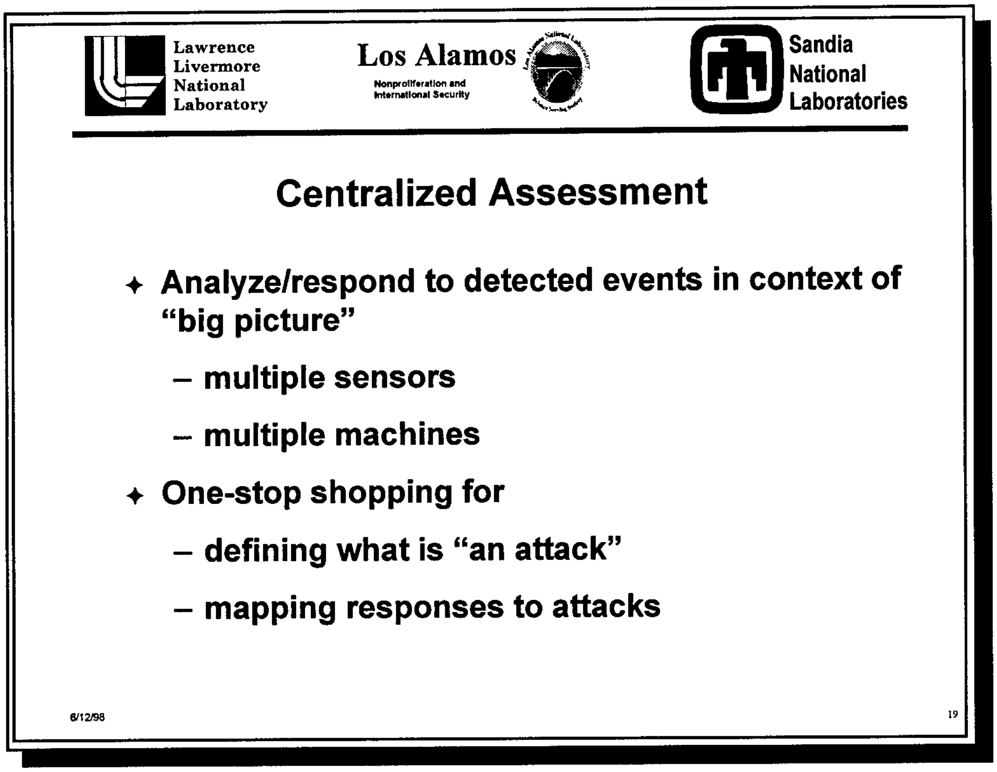


Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

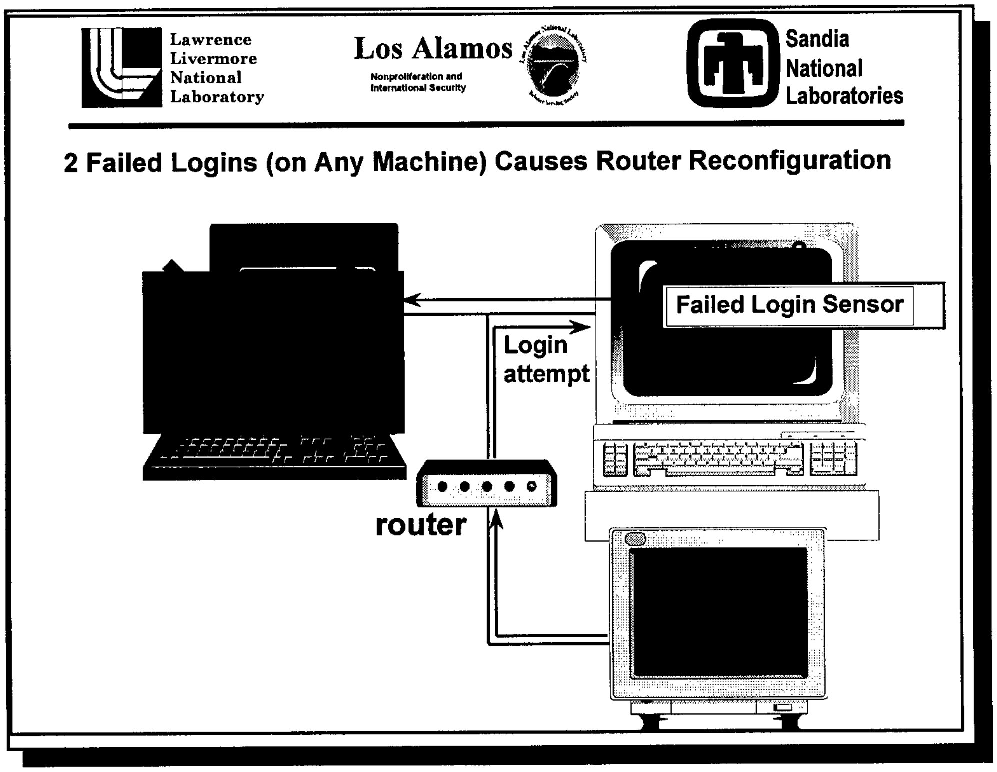
Sandia National Laboratories

The System Detects File Modification, Ejects the Intruder

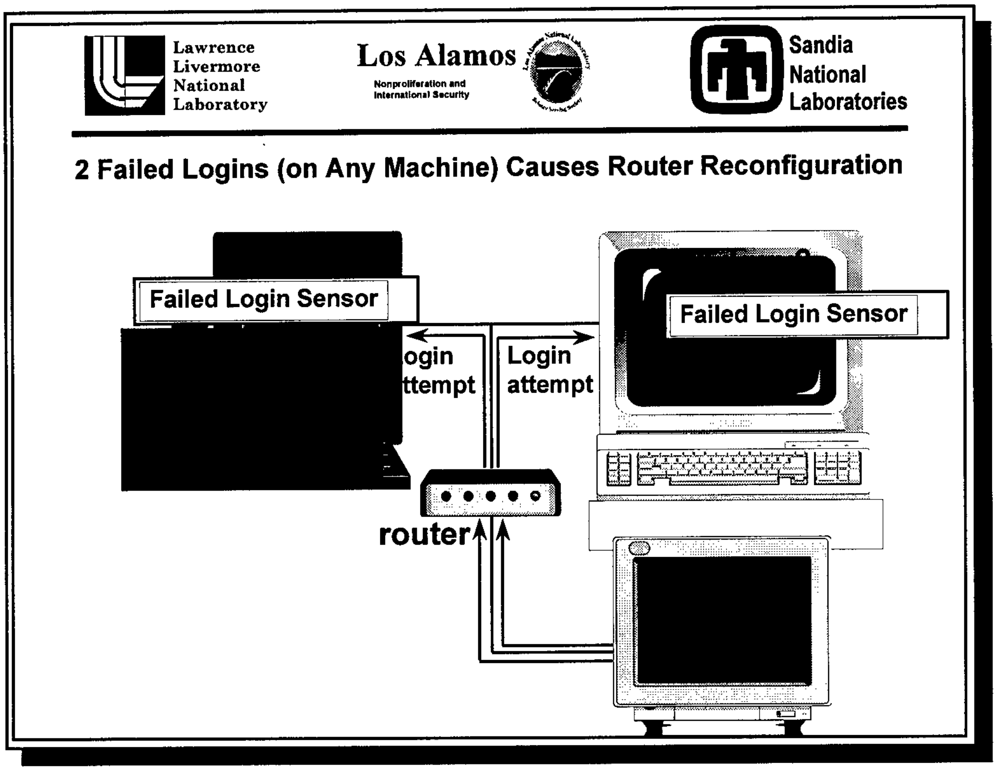


Centralized Assessment

- Analyze/respond to detected events in context of "big picture"
  - multiple sensors
  - multiple machines
- One-stop shopping for
  - defining what is "an attack"
  - mapping responses to attacks



2 Failed Logins (on Any Machine) Causes Router Reconfiguration

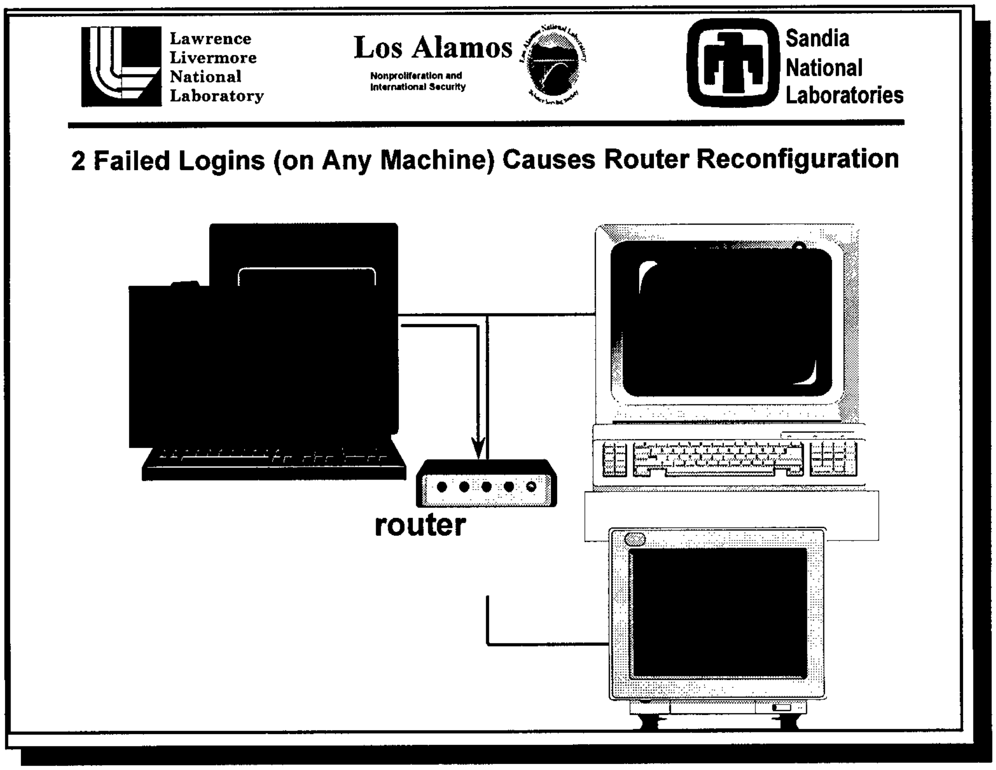


Lawrence
Livermore
National
Laboratory

Los Alamos
Nonproliferation and
International Security

Sandia
National
Laboratories

2 Failed Logins (on Any Machine) Causes Router Reconfiguration



Lawrence
Livermore
National
Laboratory

Los Alamos
Nonproliferation and
International Security

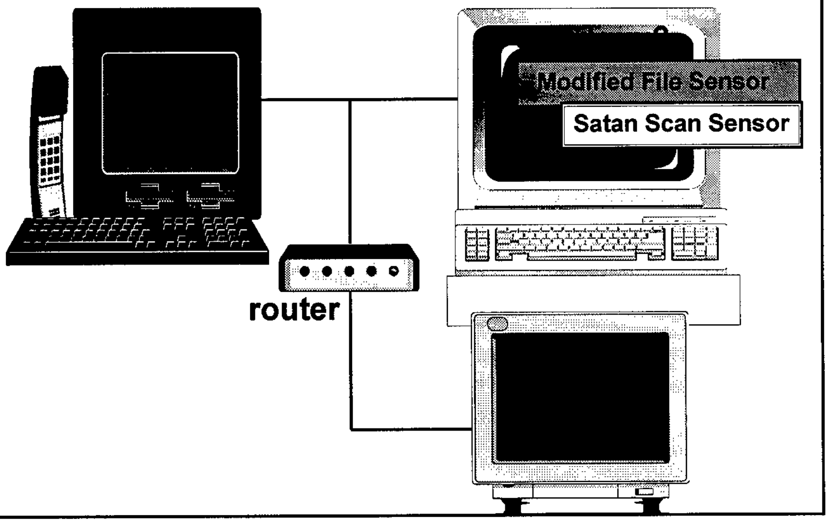
Sandia
National
Laboratories

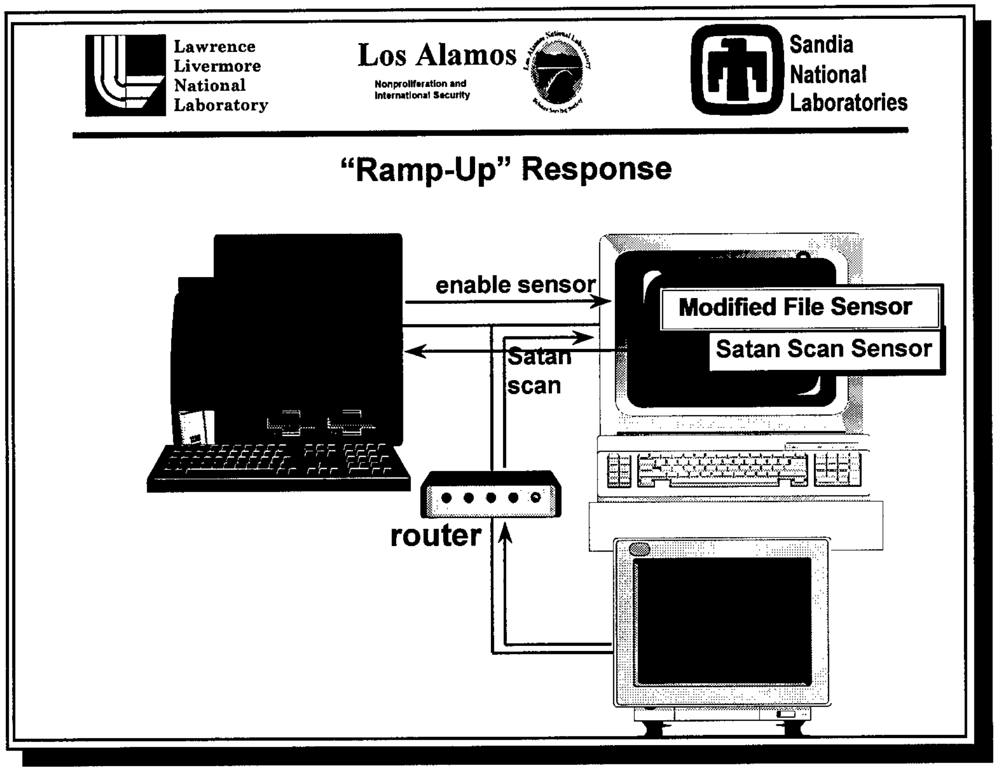
2 Failed Logins (on Any Machine) Causes Router Reconfiguration

“Ramp-Up” Detection and Response

- Disable some sensors to conserve resources
- Enable early-warning sensors
- As early-warning sensors are tripped, enable more sensors to verify attack

“Ramp-Up” Response





Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

"Ramp-Up" Response

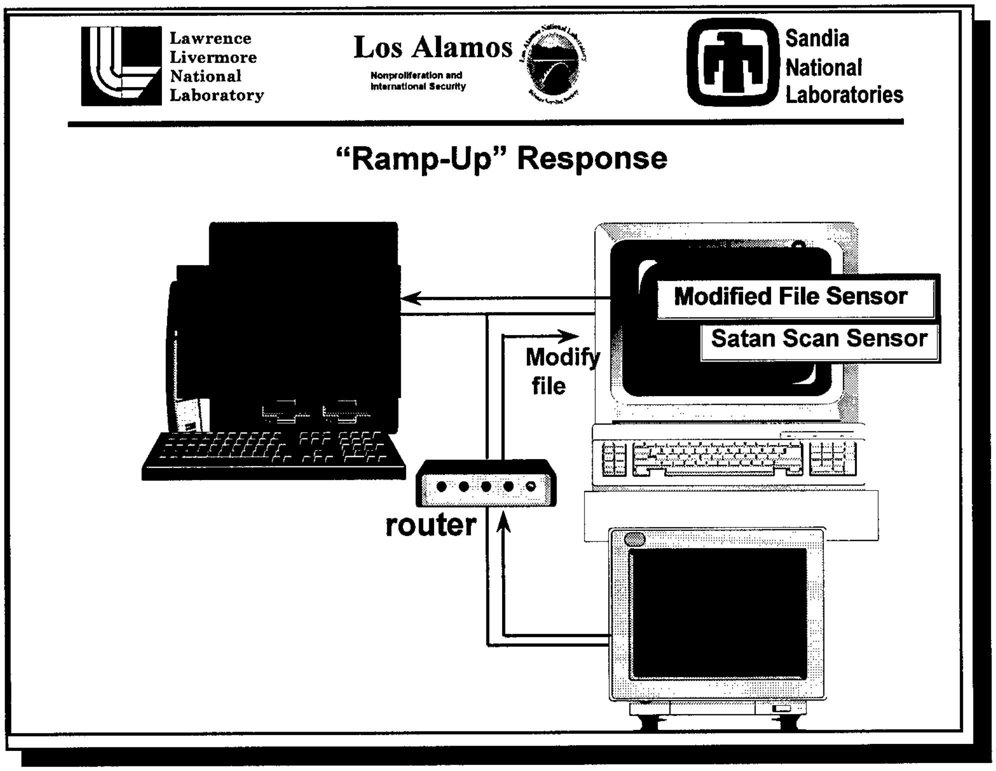
enable sensor

Modified File Sensor

Satan Scan Sensor

Satan scan

router



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

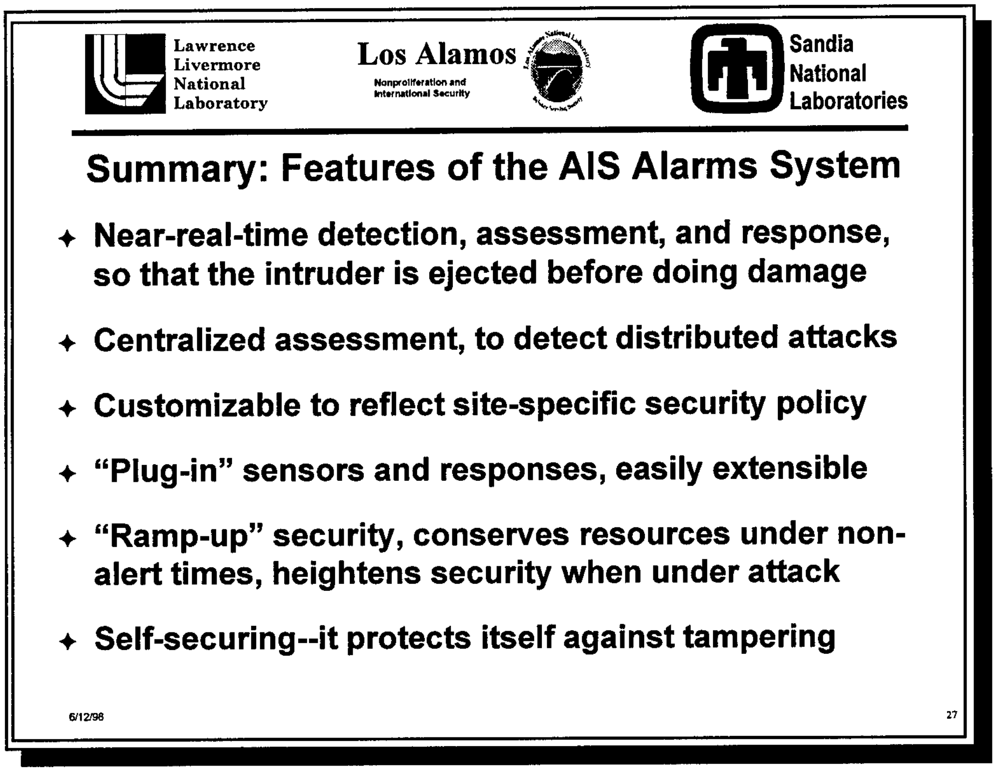
"Ramp-Up" Response

Modified File Sensor

Satan Scan Sensor

Modify file

router



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

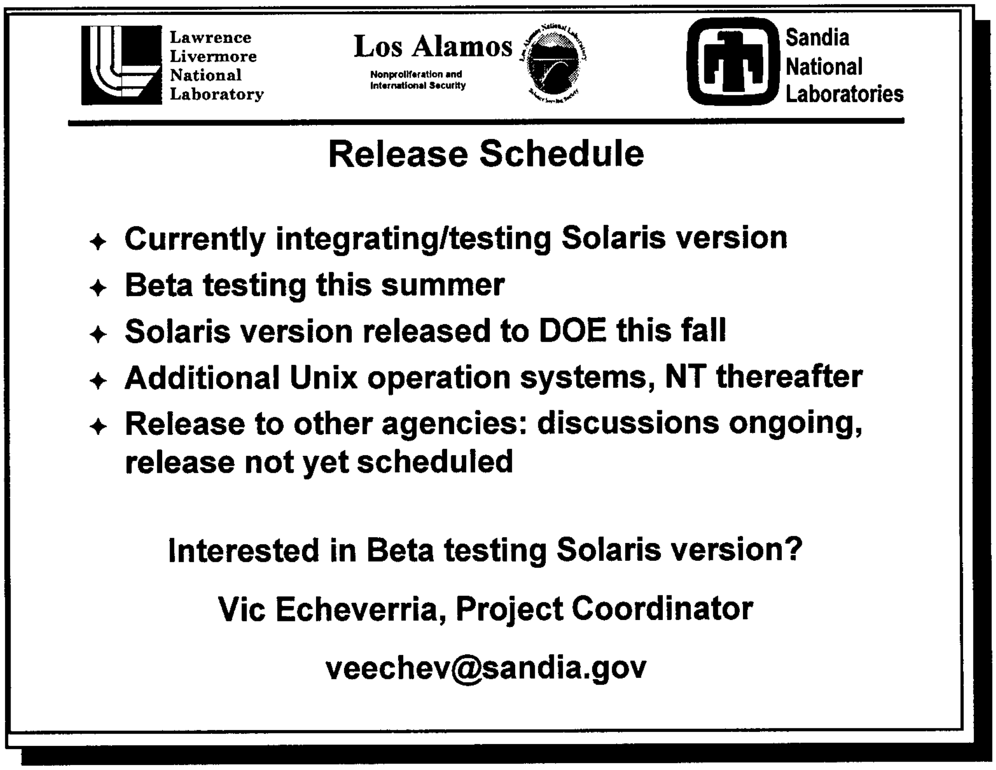
Sandia National Laboratories

Summary: Features of the AIS Alarms System

- Near-real-time detection, assessment, and response, so that the intruder is ejected before doing damage
- Centralized assessment, to detect distributed attacks
- Customizable to reflect site-specific security policy
- "Plug-in" sensors and responses, easily extensible
- "Ramp-up" security, conserves resources under non-alert times, heightens security when under attack
- Self-securing--it protects itself against tampering

6/12/98

27



Lawrence Livermore National Laboratory

Los Alamos
Nonproliferation and International Security

Sandia National Laboratories

Release Schedule

- Currently integrating/testing Solaris version
- Beta testing this summer
- Solaris version released to DOE this fall
- Additional Unix operation systems, NT thereafter
- Release to other agencies: discussions ongoing, release not yet scheduled

Interested in Beta testing Solaris version?

Vic Echeverria, Project Coordinator

veechev@sandia.gov